TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application No.	10/749,744
Filing Date	December 30, 2003
First Named Inventor	Yang Seo Choi
Art Unit	
Examiner Name	
Total Number of Pages in This Submission: 6	Attorney Docket Number: 2013P146

ENCLOSURES ***(check all that apply)***

- ☒ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Response
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
  - ☐ PTO/SB/08
- ☒ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Basic Filing Fee
  - ☐ Declaration/POA
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s)
- ☐ After Allowance Communication to Group
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) *(please identify below):*

Request for Priority; return postcard

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Eric S. Hyman, Reg. No. 30,139 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Signature	
Date	2/17/04

CERTIFICATE OF MAILING/TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Typed or printed name	Melissa Stead		
Signature	Melissa Stead	Date	2-17-04

Based on PTO/SB/21 (02-04) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 02/10/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

FEE TRANSMITTAL for FY 2004

Effective 01/01/2004. Patent fees are subject to annual revision.

☒ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT ($)

Complete if Known	
Application Number	10/749,744
Filing Date	December 30, 2003
First Named Inventor	Yang Seo Choi
Examiner Name	
Art Unit	
Attorney Docket No.	2013P146

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account

Deposit Account Number: 02-2666

Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

The Commissioner is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☐ Credit any overpayments

☒ Charge any additional fee(s) or underpayment of fees as required under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20.

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES

		Extra Claims		Fee from below	Fee Paid
Total Claims	- 20** =		X		=
Independent Claims	- 3 =		X		=
Multiple Dependent					=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple Dependent claim, if not paid
1204	86	2204	43	**Reissue independent claims over original patent
1205	18	2205	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)

***or number previously paid, if greater, For Reissues, see below*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920 *	1804	920 *	Requesting publication of SIR prior to Examiner action	
1805	1,840 *	1805	1,840 *	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	1,210	2255	605	Extension for reply within fifth month	
1404	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	1809	385	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($)

SUBMITTED BY

Complete (if applicable)

Name (Print/Type)	Eric S. Hyman	Registration No. (Attorney/Agent)	30,139	Telephone	(310) 207-3800
Signature				Date	2/17/04

Based on PTO/SB/17 (10-03) as modified by Blakely, Sokoloff, Taylor & Zafman (wir) 02/10/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

DOCKET NO.: 2013P146

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

YANG SEO CHOI, ET AL.

Application No.: 10/749,744

Filed: December 30, 2003

For: **Apparatus and Method for Providing Real-Time Traceback Connection Using Connection Redirection Technique**

Art Group:

Examiner:

Commissioner for Patents
P.O, Box 1450
Alexandria, VA 22313-1450

REQUEST FOR PRIORITY

Applicant respectfully requests a convention priority for the above-captioned application, namely:

COUNTRY	APPLICATION NUMBER	DATE OF FILING
Republic of Korea	2003-64573	17 September 2003

☒ A certified copy of the document is being submitted herewith.

Respectfully submitted,
Blakely, Sokoloff, Taylor & Zafman LLP

Dated: 2/17/04

Eric S. Hyman, Reg. No. 30,139

12400 Wilshire Boulevard, 7th Floor
Los Angeles, CA 90025
Telephone: (310) 207-3800

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Melissa Stead 2-17-04

Melissa Stead *Date*

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0064573
Application Number

출 원 년 월 일 : 2003년 09월 17일
Date of Application SEP 17, 2003

출 원 인 : 한국전자통신연구원
Applicant(s) Electronics and Telecommunications Research Insi

2003 년 12 월 23 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0015
【제출일자】	2003.09.17
【국제특허분류】	H04L
【발명의 명칭】	연결 재설정 기법을 이용한 실시간 연결 역추적 장치 및 그 방법
【발명의 영문명칭】	Apparatus and method for providing a real-time connection traceback using connection redirection technique
【출원인】	
【명칭】	한국전자통신연구원
【출원인코드】	3-1998-007763-8
【대리인】	
【성명】	이영필
【대리인코드】	9-1998-000334-6
【포괄위임등록번호】	2001-038378-6
【대리인】	
【성명】	이해영
【대리인코드】	9-1999-000227-4
【포괄위임등록번호】	2001-038396-8
【발명자】	
【성명의 국문표기】	최양서
【성명의 영문표기】	CHOI,Yang Seo
【주민등록번호】	731121-1318719
【우편번호】	305-751
【주소】	대전광역시 유성구 송강동 송강그린아파트 316동 1004호
【국적】	KR
【발명자】	
【성명의 국문표기】	서동일
【성명의 영문표기】	SEO,Dong Il
【주민등록번호】	620221-1648317

【우편번호】 305-761
【주소】 대전광역시 유성구 전민동 464-1 엑스포아파트 107동 501호
【국적】 KR
【발명자】
【성명의 국문표기】 김환국
【성명의 영문표기】 KIM,Hwan Kuk
【주민등록번호】 730114-1524321
【우편번호】 135-795
【주소】 서울특별시 강남구 역삼2동 개나리아파트 24동 505호
【국적】 KR
【발명자】
【성명의 국문표기】 이상호
【성명의 영문표기】 LEE,Sang Ho
【주민등록번호】 530315-1069629
【우편번호】 361-302
【주소】 충청북도 청주시 흥덕구 봉명2동 세원아파트 101동 1107호
【국적】 KR

【공지예외적용대상증명서류의 내용】
【공개형태】 간행물 발표
【공개일자】 2003.07.25

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
이영필 (인) 대리인
이해영 (인)

【수수료】

【기본출원료】	20 면	29,000 원
【가산출원료】	6 면	6,000 원
【우선권주장료】	0 건	0 원
【심사청구료】	14 항	557,000 원
【합계】	592,000 원	
【감면사유】	정부출연연구기관	
【감면후 수수료】	296,000 원	

【기술이전】

【기술이전】

【기술양도】	희망
【실시권 허여】	희망
【기술지도】	희망
【첨부서류】	1. 요약서·명세서(도면)_1통 2.공지예외적용대상(신규성상실의예외, 출원시의특례)규정을 적용받 기 위한 증명서류_1통

【요약서】

【요약】

연결 재설정기법을 이용한 연결 역추적 장치 및 그 방법이 개시된다. 패킷차단부는 시스템 공격감지신호를 수신하면, 시스템으로 전송되는 공격패킷 및 공격패킷에 대한 응신으로 시스템으로부터 출력되는 제1응답패킷을 차단한다. 응답패킷생성부는 공격패킷에 대한 응신으로 워터마크를 삽입한 제2응답패킷을 생성하여 공격패킷의 근원지 주소에 해당하는 시스템으로 전송한다. 경로 역추적부는 제2응답패킷의 전송경로상에 존재하는 시스템으로부터 제2응답패킷의 전송경로정보를 포함하는 탐지패킷을 수신하고, 수신한 탐지패킷을 기초로 제2응답패킷의 전송경로를 역추적하여 공격자시스템의 위치를 파악한다. 본 발명에 따르면, 공격자가 여러 시스템을 경유하여 특정 시스템을 공격하더라도 신속하고 정확하게 공격자 시스템의 실제 위치를 추적할 수 있으며, 공격받는 시스템의 피해를 최소화 할 수 있다.

【대표도】

도 2

【색인어】

공격 패킷, 응답 패킷, 워터마크, 역추적

【명세서】

【발명의 명칭】

연결 재설정 기법을 이용한 실시간 연결 역추적 장치 및 그 방법{Apparatus and method for providing a real-time connection traceback using connection redirection technique}

【도면의 간단한 설명】

도 1은 종래의 시스템 공격과정의 일 예를 도시한 도면,

도 2는 본 발명에 따른 역추적 장치의 구성을 도시한 블록도,

도 3은 본 발명에 따른 역추적 과정을 본 발명에 따른 역추적 장치의 구성을 중심으로 도시한 도면,

도 4는 본 발명에 따른 역추적 장치를 구비한 네트워크에서 공격자시스템의 역추적과정을 도시한 도면,

도 5는 본 발명에 따른 역추적 방법의 흐름을 도시한 흐름도, 그리고,

도 6은 본 발명에 따른 역추적 장치에서 워터마크 탐지방법의 흐름을 도시한 흐름도이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<7> 본 발명은 네트워크에서 공격자시스템의 위치를 추적하는 장치에 관한 것으로, 보다 상세하게는, 공격자시스템과의 실시간 연결을 기초로 공격자시스템의 위치를 추적하는 역추적시스템에 관한 것이다.

<8> 연결 역추적(connection traceback) 기술은 해킹을 시도하는 해커의 실제 위치를 실시간으로 추적하는 기술을 의미하는 것으로서, 종래의 연결 역추적 기술에는 크게 IP 패킷 역추적 기술과 TCP 연결 역추적 기술이 있다. IP 패킷 역추적 기술은 IP 주소가 변경된 패킷의 실제 송신지를 추적하는 기술이고, TCP 연결 역추적 기술은 다수의 중간 경유 시스템을 이용하여 해킹을 시도하는 해커의 현재 위치를 추적하는 기술로서 흔히 연결 사슬(Connection Chain) 역추적 기술이라고 불린다.

<9> 종래의 역추적 기술은 인터넷상에 존재하는 모든 호스트들에 대해 역추적 모듈을 설치하거나, 네트워크 상에 송수신되는 모든 패킷과 중간 경유 시스템의 연결에 대한 정보를 모두 수집 기록하여야 이용가능하다. 그러나, 인터넷 환경에서 이러한 요건을 모두 충족시키기에는 현실성이 떨어질 뿐만 아니라, 원하는 모든 대상 시스템에 역추적 기능을 설치한다고 하여도 공격자도 경유한 중간 경유 시스템들 중 어느 하나의 시스템에서 여러 원인으로 인해 역추적에 필요한 정보를 얻을 수 없다면 역추적이 불가능한다.

<10> 도 1은 종래의 시스템 공격과정의 일 예를 도시한 도면이다.

<11> 도 1을 참조하면, 제1네트워크에 속한 공격자(100)가 1차공격을 통해 제2네트워크에 속한 제1피해시스템(110)을 공격하고, 공격을 통해 획득한 제1피해시스템의 특정 권한을 이용하여 최종 공격 목표인 제3네트워크의 제2피해시스템(120)을 공격한다.

<12> 중간 경유 시스템(제1피해시스템)(110)은 하나 이상이 존재할 수 있으며, 공

격자로부터 제1피해시스템(110)으로의 접근이 공격에 의한 침입이 아니라 정상적이 방법을 통해 접근한 후 최종 목표인 제2피해시스템(120)을 공격할 수 있다. 이런 경우에, 제2피해시스템(120)은 직접적으로 실제 공격자가 위치한 시스템에 대한 정보를 얻을 수 없으며, 일반적으로 공격자에 대한 정보를 얻기 위해서는 제1피해시스템(110)에 대한 정말한 조사가 필요하다. 따라서, 최종 피해시스템(제2피해시스템)(120)이 다수의 중간 경유 시스템(제1피해시스템)(110)중 어느 하나의 중간 경유 시스템에서 추적에 필요한 정보를 얻을 수 없다면 추적은 더 이상 불가능하다.

【발명이 이루고자 하는 기술적 과제】

<13> 본 발명이 이루고자 하는 기술적 과제는, 해커로부터 공격당하는 피해시스템의 피해를 최소화하고, 공격자시스템의 위치를 정확하고 신속하게 역추적하는 연결 역추적시스템 및 그 방법을 제공하는 데 있다.

<14> 본 발명이 이루고자 하는 다른 기술적 과제는, 해커로부터 공격당하는 피해시스템의 피해를 최소화하고, 공격자시스템의 위치를 정확하고 신속하게 역추적하는 연결 역추적방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는 데 있다.

【발명의 구성 및 작용】

<15> 상기의 기술적 과제를 달성하기 위한, 본 발명에 따른 역추적 장치의 일 실시예는, 시스템 공격감지신호를 수신하면, 상기 시스템으로 전송되는 공격패킷 및 상기 공격패킷에 대한 응신으로 상기 시스템으로부터 출력되는 제1응답패킷을 차단하는 패킷차단부; 상기 공격패킷에 대한 응신으로 워터마크를 삽입한 제2응답패킷을 생성하여 상기 공격패킷의 근원지 주소에 해

당하는 시스템으로 전송하는 응답패킷생성부; 및 상기 제2응답패킷의 전송경로상에 존재하는 시스템으로부터 상기 제2응답패킷의 전송경로정보를 포함하는 탐지패킷을 수신하고, 상기 수신한 탐지패킷을 기초로 상기 제2응답패킷의 전송경로를 역추적하여 공격자시스템의 위치를 파악하는 경로 역추적부;를 갖는다.

<16> 상기의 기술적 과제를 달성하기 위한, 본 발명에 따른 역추적 방법의 일 실시예는, (a) 시스템 침입신호를 수신하면, 상기 시스템으로 전송되는 공격패킷 및 상기 공격패킷에 대한 응신으로 상기 시스템으로부터 출력되는 제1응답패킷을 차단하는 단계; (b) 상기 공격패킷에 대한 응신으로 워터마크를 삽입한 제2응답패킷을 생성하여 상기 공격패킷의 근원지 주소로 전송하는 단계; 및 (c) 상기 제2응답패킷의 전송경로상에 존재하는 시스템으로부터 상기 제2응답패킷의 전송경로정보를 포함하는 탐지패킷을 수신하고, 상기 탐지패킷을 기초로 상기 제2응답패킷의 전송경로를 역추적하여 상기 공격자시스템의 위치를 파악하는 단계;를 갖는다.

<17> 본 발명에 따르면, 공격자가 여러 시스템을 경유하여 특정 시스템을 공격하더라도 신속하고 정확하게 공격자 시스템의 실제 위치를 추적할 수 있으며, 공격받는 시스템의 피해를 최소화 할 수 있다.

<18> 이하에서, 첨부된 도면들을 참조하여 본 발명에 따른 역추적 장치 및 그 방법에 대하여 상세히 설명한다.

<19> 도 2는 본 발명에 따른 역추적 장치의 구성을 도시한 블록도이다.

<20> 도 2를 참조하면, 본 발명에 따른 역추적 장치는 공격 탐지부(200), 패킷 차

단부(210), 응답패킷 생성부(220), 경로 역추적부(230) 및 워터마크 탐지부(240)로 구성된다. 패킷차단부(210)는 수신부(212), 패킷 파악부(214) 및 차단부(216)로 구성되며, 워터마크 탐지부(240)는 탐지부(242), 탐지패킷 생성부(244), 패킷 전송부(246)로 구성된다.

<21> 공격 탐지부(200)는 외부 공격자에 의한 피해시스템의 공격을 감지한다. 공격 탐지부(200)는 본 발명에 따른 역추적 장치에 포함되어 구성되거나, 별도의 공격 탐지시스템으로 구현될 수 있다. 별도의 공격 탐지 시스템으로 구현하는 경우에는 종래의 공격 탐지시스템을 그대로 이용할 수 있다. 외부 공격자는 정당하지 않는 방법으로 시스템의 특정권한 또는 정보를 획득하기 위하여 피해시스템을 공격하는 자이다.

<22> 공격 탐지부(200)는 피해 시스템에 대한 공격을 감지하면, 피해시스템의 공격 경로을 파악한다. 파악된 공격경로의 근원지 및 목적지 IP 주소와 포트번호를 파악하고, 파악된 IP 주소와 포트번호를 공격감지신호에 포함하여 출력한다. 공격자는 일반적으로 중간 경유 시스템을 이용하여 최종 공격 대상 시스템을 공격한다. 따라서, 공격 탐지부(200)에 의해 파악되는 공격경로는 피해 시스템과 연결된 중간 경유 시스템사이의 경로이다. 따라서 피해 시스템은 직접 공격자의 시스템 위치를 알 수 없다.

<23> 공격탐지부(200)는 피해 시스템의 로그파일, 피해시스템과 연결된 네트워크의 로그 파일, 피해 시스템의 특정 시스템 파일의 변경여부 등을 조사하여 상기 외부공격자에 의한 시스템 공격을 감지하고, 상기 시스템의 로그 파일을 기초로 공격패킷의 근원지 IP 주소 및 포트번호를 파악할 수 있다.

<24> 패킷 차단부(210)는 공격 탐지부(200)에 의해 피해시스템의 공격감지신호를 수신하면, 공격패킷 및 응답패킷을 차단한다. 공격패킷은 외부공격자가 피해시스템 공격을 위하여 피해시스템으로 전송하는 패킷이고, 응답패킷은 공격을 받는 피해 시스템에서 외부공격자로 전송되

는 공격패킷에 대한 응신이다. 패킷 차단부(210)에 의해 공격자의 공격패킷과 공격받는 피해시스템의 응답패킷이 차단되므로 본 발명에 따른 역추적 수행중에 피해 시스템은 더 이상 공격자에 의해 피해를 입지 않는다.

<25> 패킷 차단부(210)는 구체적으로 수신부(212), 패킷 파악부(214) 및 차단부(216)를 포함하고, 이하에서 패킷 차단부(210)의 각 구성을 중심으로 상세히 설명한다.

<26> 수신부(212)는 공격 탐지부(200)로부터 피해시스템의 공격감지신호를 수신한다. 공격감지신호는 공격 경로의 근원지 및 목적지의 IP 주소와 포트번호를 포함한다.

<27> 패킷 파악부(214)는 수신부(212)에 의해 수신된 근원지 및 목적지의 IP 주소와 포트번호를 기초로 피해시스템으로 송수신되는 패킷 중 공격패킷 및 공격패킷에 대한 응신인 응답패킷을 파악한다. 예를 들어, 피해 시스템으로 전송되는 패킷의 근원지 및 목적지의 IP 주소와 포트번호가 수신부(212)에 의해 수신된 IP 주소 및 포트번호와 동일하면 이 패킷은 공격패킷이다. 즉, IP 주소를 기초로 공격 경로의 양단을 파악하고 양단 사이에 송수신되는 패킷 중 포트번호를 기초로 공격 패킷 및 응답 패킷을 파악한다.

<28> 차단부(216)는 패킷 파악부(214)에 의해 파악된 공격패킷 및 응답패킷을 중간에서 차단하여 더 이상 피해시스템이 공격자에 의해 피해를 입지 않도록 한다.

<29> 응답패킷 생성부(220)는 패킷 차단부(210)에 의해 차단된 공격패킷에 대한 응신으로 직접 응답패킷을 생성한다. 응답패킷 생성부는(220) 공격자에 의한 공격패킷을 도중에서 가로채고 응답패킷을 생성하여 전송하므로, 공격자시스템과 피해시스템과의 연결을 공격자시스템과 추적 장치의 연결로 변경하는 연결 재설정기능을 수행한다. 응답패킷 생성부(220)는 응답패킷

에 응답패킷의 전송경로를 역추적 할 수 있는 워터마크(watermark)를 삽입한다. 응답패킷 생성부(220)는 워터마크를 삽입한 응답패킷을 공격패킷의 근원지 IP 주소로 전송한다.

<30> 응답패킷은 네트워크의 여러 경로를 거쳐 최종적으로 외부공격자의 시스템으로 전달된다. 따라서, 외부공격자가 연결을 유지하는 공격 즉, TCP 연결을 통한 공격을 하는 경우에 공격패킷에 대한 응답패킷은 여러 시스템을 경유하여 공격자 시스템의 실제 위치까지 전송되므로, 소정의 경로추적 데이터를 삽입한 응답패킷을 이용하여 공격자의 실제위치를 역추적할 수 있다.

<31> 워터마크(watermark)는 어떤 파일에 관한 저작권 정보(즉 저자 및 권리 등)를 식별할 수 있도록 디지털 이미지나 오디오 및 비디오 파일에 삽입한 비트 패턴을 말한다. 이 용어는 편지지의 제작회사를 나타내기 위해 희미하게 프린트된 투명무늬(이것을 영어로 '워터마크'라고 한다)로부터 유래되었다. 의도적으로 어느 정도까지는 볼 수 있도록 만든 프린트 워터마크와는 달리, 디지털 워터마크는 완전히 안보이게(저작물이 오디오인경우에는 안 들리게) 설계된다. 워터마크를 나타내는 실제 비트들은 그것들이 식별되거나 조작되지 않도록 파일 전체에 걸쳐 퍼져 있다. 워터마크를 보기 위해서는, 워터마크 데이터를 추출하는 방법을 알고 있는 특수한 프로그램이 필요하다.

<32> 워터마크 탐지부(240)는 외부로부터 수신한 패킷 속에 워터마크가 포함되어 있는지 탐지한다. 워터마크 탐지부(240)는 워터마크가 포함된 패킷을 탐지하면, 패킷의 근원지 및 목적지 IP 주소와 포트번호를 포함하는 탐지패킷을 생성한다. 그리고, 워터마크 탐지부(240)는 생성한 탐지패킷을 최초로 워터마크를 패킷에 삽입한 시스템으로 전송한다. 최초로 워터마크를 패킷에 삽입한 시스템은 탐지패킷을 수신하고 탐지패킷에 포함된 IP 주소와 포트번호를 기초로 경

로를 역추적하여 공격자 시스템의 위치를 파악한다. 워터마크 탐지부(240)는 역추적 장치의 다른 구성요소와 독립적으로 설치되어 운용될 수 있다.

<33> 워터마크 탐지부(240)는 구체적으로 탐지부(242), 탐지패킷 생성부(244) 및 패킷전송부(246)로 구성된다.

<34> 탐지부(242)는 수신한 패킷에 워터마크가 포함되어 있는지를 탐지한다. 탐지부(242)는 워터마크를 추출할 수 있는 특수한 프로그램을 포함하고 있으며, 이 프로그램에 의해 패킷속에 포함된 워터마크를 탐지된다.

<35> 탐지패킷 생성부(244)는 탐지부(242)가 워터마크가 포함된 패킷을 탐지하면 패킷의 근원지 및 목적지 IP 주소와 포트번호를 포함하는 탐지패킷을 생성한다. 탐지패킷은 이 외에 경로 추적을 위한 정보를 더 포함할 수 있다.

<36> 패킷 전송부(246)는 워터마크를 패킷에 최초로 삽입한 시스템으로 탐지패킷 생성부(244)에 의해 생성된 탐지패킷을 전송한다. 워터마크를 패킷에 최초로 삽입한 시스템의 정보는 패킷속에 포함되어 있다.

<37> 경로 역추적부(230)는, 응답패킷 생성부(220)가 생성하여 전송한 응답패킷에 대한 응신으로, 네트워크에 설치된 다른 역추적장치로부터 탐지패킷을 수신한다. 경로 역추적부(230)는 탐지패킷에 포함된 IP 주소와 포트번호를 기초로 공격자 시스템의 실제 위치를 역추적한다. 예들 들어, 경로 역추적부(230)가 근원지 및 목적지 IP 주소가 addr1 및 addr2인 제1탐지패킷, addr2 및 addr3인 제2 탐지패킷을 수신하면, addr1, addr2 및 addr3인 IP 주소들을 순서대로 추적하여 응답패킷의 최종전달위치를 역추적할 수 있다.

<38> 도 3은 본 발명에 따른 역추적 과정을 본 발명에 따른 역추적 장치의 구성을 중심으로 도시한 도면이다.

<39> 도 3을 참조하면, 피해시스템(300)과 외부공격자가 속한 네트워크 사이에 역추적장치가 설치되어 있다. 역추적 장치는 공격 탐지부(310), 패킷 차단부(320), 응답패킷 생성부(330), 경로 역추적부(340) 및 워터마크 탐지부(350)로 구성된다.

<40> 공격 탐지부(310), 패킷 차단부(320), 응답패킷 생성부(330), 경로 역추적부(340) 및 워터마크 탐지부(350)의 구성과 기능은 도 2에서 설명한 것과 동일하므로 상세한 설명은 생략한다. 여기서는 연결 역추적방법의 전반적인 흐름을 위주로 살펴본다.

<41> 외부공격자에 의해 피해 시스템으로의 공격이 발생하면(S300), 공격 탐지부(310)는 피해 시스템으로의 공격을 감지한다(S305). 패킷 차단부(320)는 공격감지부(310)로부터 공격감지신호를 수신하면 공격패킷 및 응답패킷을 차단하고(S310), 수신되는 공격패킷을 응답패킷생성부(330)로 전송한다(S315). 이로써, 외부공격자는 공격에 대한 연결이 계속 유지되는 것으로 인지하고, 역추적 장치는 계속 유지되는 연결을 통하여 외부공격자의 시스템 위치를 역추적한다.

<42> 패킷 차단부(320)에 의해 공격패킷의 연결 방향이 재설정되어 공격패킷이 응답패킷 생성부(330)로 전송되면(S315), 응답패킷 생성부(330)는 공격패킷에 대한 응신으로 워터마크를 삽입한 응답패킷을 생성한다(S320). 생성된 응답패킷은 네트워크의 여러 시스템을 경유하여 최종적으로 공격자시스템으로 전송된다(S325).

<43> 경로역추적부(340)는 응답패킷을 감지한 외부시스템으로부터 전송된 탐지패킷을 기초로 응답패킷의 경로를 역추적하여 공격자시스템의 위치를 파악한다(S330). 워터마크탐지부(350)는

수신한 패킷에 워터마크가 포함되어 있다면 최초로 워터마크를 패킷에 삽입한 시스템으로 탐지 패킷을 생성하여 전송한다(S335).

<44> 도 4는 본 발명에 따른 역추적 장치를 구비한 네트워크에서 공격자시스템의 역추적과정을 도시한 도면이다.

<45> 도 4를 참조하면, 네트워크에는 공격자 시스템(400)이 속한 제1네크워크, 제1피해시스템(410)이 속한 제2네트워크 및 제2피해시스템(420)이 속한 제3네트워크가 있다. 각 네트워크는 본 발명에 따른 역추적 장치(430,440,450)를 포함하고 있다.

<46> 공격자는 제2네트워크의 제1피해시스템(410)을 경유하여 최종적으로 제3네트워크의 제2피해시스템(420)을 공격한다. 공격자는 제1피해시스템(410)을 공격하여 접속하거나, 정상적인 방법으로 제1피해시스템(410)에 접속할 수 있다.

<47> 제2피해시스템(420)이 공격자에 의해 공격을 받으면, 제3역추적 장치(450)는 제2피해시스템(420)으로부터 출력되는 응답패킷을 차단하고, 자체적으로 워터마크를 포함한 응답패킷을 생성하여 전송한다. 워터마크를 포함한 응답패킷은 제1피해시스템(410)을 경유하여 공격자시스템으로 전달된다.

<48> 워터마크를 포함한 응답패킷을 수신한 제2역추적 장치(440)는 응답패킷의 IP 주소와 포트번호를 포함한 탐지패킷을 생성하고, 이를 제3역추적 장치(450)로 전송한다.

<49> 워터마크를 포함한 응답패킷은 제2역추적 장치(440)를 경유하여 제1역추적장치(430)로 전송된다. 워터마크를 포함한 응답패킷을 수신한 제1역추적 장치(430)는 탐지패킷을 생성하고, 생성한 탐지패킷을 제3역추적 장치(450)로 전송한다.

<50> 제3역추적 장치(450)는 제1역추적 장치(440) 및 제2역추적 장치(430)로부터 패킷의 근원지 및 목적지의 IP 주소와 포트번호를 포함하는 탐지패킷을 수신한다. 제3역추적 장치(450)는 수신한 두개의 탐지패킷의 IP 주소 및 포트번호를 기초로 응답패킷의 전송경로를 역추적하여 최종적으로 응답패킷이 전달된 시스템의 IP 주소를 파악할 수 있다. 이로써, 공격자시스템의 위치를 역추적할 수 있다.

<51> 도 5는 본 발명에 따른 역추적 방법의 흐름을 도시한 흐름도이다.

<52> 도 5를 참조하면, 공격 탐지부(200)는 외부공격자에 의한 시스템의 공격을 감지하고, 공격 경로의 근원지 및 목적지 IP 주소와 포트번호를 포함하는 공격감지신호를 출력한다(S500). 공격탐지부(200)는 종래의 공격감지시스템을 사용할 수 있으며, 본 발명에 따른 역추적 장치에 포함되어 구현되거나, 독립적으로 구현될 수 있다.

<53> 패킷차단부(210)는 공격감지신호를 수신하면, 시스템으로 전송되는 공격패킷 및 공격패킷에 대한 응신으로 시스템으로부터 출력되는 응답패킷을 차단한다(S510). 공격패킷 및 응답패킷은 공격 경로의 IP 주소 및 포트번호를 기초로 파악된다.

<54> 응답패킷 생성부(220)는 공격패킷에 대한 응신으로 워터마크를 삽입한 응답패킷을 생성하여 공격자 시스템으로 전송한다(S520). 워터마크를 삽입한 응답패킷은 일반적으로 여러 시스템을 경유하여 공격자 시스템에 전송된다.

<55> 경로 역추적부(230)는 외부 시스템으로부터 하나이상의 워터마크 탐지패킷을 수신하고(S530), 수신한 탐지패킷에 포함된 IP 주소 및 포트번호를 기초로 응답패킷의 전송경로를 역추적하여 공격자시스템의 실제 위치를 파악한다(S540).

<56> 도 6은 본 발명에 따른 역추적 시스템에서 워터마크를 포함하는 응답패킷을 탐지하는 방법의 흐름을 도시한 도면이다.

<57> 도 6을 참조하면, 역추적 시스템은 외부시스템으로부터 패킷을 수신한다(S600). 워터마크 탐지부(240)는 워터마크를 추출할 수 있는 특별한 프로그램을 포함하고 있으며, 이 프로그램을 이용하여 수신한 패킷에 워터마크가 포함되어 있는지 파악한다(S610).

<58> 패킷에 워터마크가 포함되어 있다면(S610), 워터마크 탐지부(240)는 수신한 패킷의 근원지 및 목적지 IP 주소와 포트번호를 포함하는 탐지패킷을 생성한다(S620). 워터마크 탐지부(240)는 패킷에 워터마크를 최초로 삽입한 시스템으로 생성한 탐지패킷을 전송한다(S630).

<59> 워터마크를 최초로 삽입한 시스템은 네트워크의 시스템들로부터 탐지패킷을 수신하면 탐지패킷에 포함된 IP 주소와 포트번호를 기초로 경로를 역추적하여 공격자시스템의 위치를 파악한다.

<60> 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

<61> 이상의 설명은 바람직한 실시예를 설명한 것에 불과한 것으로서, 본 발명은 상술한 실시예에 한정되지 아니하며 첨부한 특허청구범위 내에서 다양하게 변경 가능하다. 예를 들어 본

발명의 실시예에 구체적으로 나타난 각 구성요소의 형상 및 구조는 변형하여 실시 할 수 있다.

【발명의 효과】

<62> 본 발명에 따르면, 공격자가 여러 시스템을 경유하여 특정 시스템을 공격하더라도 신속하고 정확하게 공격자 시스템의 실제 위치를 추적할 수 있다. 공격자에 의한 특정 시스템의 공격을 감지하면 공격패킷 및 응답패킷을 차단하므로 공격자에 의한 시스템의 피해를 최소화하면서 공격자의 위치 추적을 할 수 있다.

<63> 종래의 역추적 시스템이 여러 중간 경유 시스템 중 어느 하나로부터 필요한 정보를 수집하지 못하면 추적을 할 수 없는데 반해, 본 발명에 따른 역추적 시스템은 여러 중간 경유 시스템 중 어느 하나로부터 필요한 정보를 얻지 못한 경우에도 공격자시스템의 위치 추적이 가능하다.

【특허청구범위】

【청구항 1】

시스템 공격감지신호를 수신하면, 상기 시스템으로 전송되는 공격패킷 및 상기 공격패킷에 대한 응신으로 상기 시스템으로부터 출력되는 제1응답패킷을 차단하는 패킷차단부;

상기 공격패킷에 대한 응신으로 워터마크를 삽입한 제2응답패킷을 생성하여 상기 공격패킷의 근원지 주소에 해당하는 시스템으로 전송하는 응답패킷생성부; 및

상기 제2응답패킷의 전송경로상에 존재하는 시스템으로부터 상기 제2응답패킷의 전송경로정보를 포함하는 탐지패킷을 수신하고, 상기 수신한 탐지패킷을 기초로 상기 제2응답패킷의 전송경로를 역추적하여 공격자시스템의 위치를 파악하는 경로 역추적부;를 포함하는 것을 특징으로 하는 연결 역추적 장치.

【청구항 2】

제 1항에 있어서,

외부공격자에 의한 시스템 공격을 감지하면, 상기 공격 경로의 근원지 및 목적지 IP 주소와 포트번호를 포함하는 공격감지신호를 출력하는 공격탐지부를 더 포함하는 것을 특징으로 하는 연결 역추적 장치.

【청구항 3】

제 2항에 있어서,

상기 공격탐지부는,

상기 시스템의 로그파일, 네트워크의 로그 파일, 특정 시스템 파일의 변경여부 등을 조사하여 상기 외부공격자에 의한 시스템 공격을 감지하고, 상기 시스템의 로그 파일을 기초로 공격패킷의 근원지 IP 주소 및 포트번호를 파악하는 것을 특징으로 하는 연결 역추적 장치.

【청구항 4】

제 2항에 있어서,

상기 패킷차단부는,

상기 공격감지신호를 수신하는 신호수신부;

상기 IP 주소 및 상기 포트번호를 기초로 상기 공격 패킷 및 상기 제1응답패킷을 파악하는 패킷파악부; 및

상기 공격패킷 및 상기 제1응답패킷을 차단하는 차단부;를 포함하는 것을 특징으로 하는 연결 역추적 장치.

【청구항 5】

제 1항에 있어서,

외부네트워크로부터 워터마크를 포함하는 패킷을 수신하면 상기 워터마크를 삽입한 외부네트워트의 시스템으로 상기 수신한 패킷의 경로정보를 포함하는 탐지패킷을 전송하는 워터마크탐지부를 더 포함하는 것을 특징으로 하는 연결 역추적 장치.

【청구항 6】

제 5항에 있어서,

상기 워터마크 탐지부는,

외부로부터 수신한 패킷에 포함된 워터마크를 탐지하는 탐지부;

상기 워터마크를 탐지하면 상기 수신한 패킷의 근원지 및 목적지 IP 주소 및 포트번호를 포함하는 탐지패킷을 생성하는 탐지패킷생성부; 및

상기 패킷에 상기 워터마크를 최초로 삽입한 시스템으로 상기 생성된 탐지패킷을 전송하는 패킷전송부;를 포함하는 것을 특징으로 하는 연결 역추적 장치.

【청구항 7】

제 1항에 있어서,

상기 경로 역추적부는,

상기 수신한 하나이상의 탐지패킷에 포함된 근원지 및 목적지 IP 주소 및 포트번호를 기초로 공격자시스템의 위치를 역추적하는 것을 특징으로 하는 연결 역추적 장치.

【청구항 8】

(a) 시스템 침입신호를 수신하면, 상기 시스템으로 전송되는 공격패킷 및 상기 공격패킷에 대한 응신으로 상기 시스템으로부터 출력되는 제1응답패킷을 차단하는 단계;

(b) 상기 공격패킷에 대한 응신으로 워터마크를 삽입한 제2응답패킷을 생성하여 상기 공격패킷의 근원지 주소로 전송하는 단계; 및

(c) 상기 제2응답패킷의 전송경로상에 존재하는 시스템으로부터 상기 제2응답패킷의 전송경로정보를 포함하는 탐지패킷을 수신하고, 상기 탐지패킷을 기초로 상기 제2응답패킷의 전송경로를 역추적하여 상기 공격자시스템의 위치를 파악하는 단계;를 포함하는 것을 특징으로 하는 연결 역추적 방법.

【청구항 9】

제 8항에 있어서,

(d) 외부공격자에 의한 시스템의 공격을 감지하면, 상기 공격 경로의 근원지 및 목적지 IP 주소와 포트번호를 포함하는 공격감지신호를 출력하는 단계를 상기 (a) 단계 전에 포함하는 것을 특징으로 하는 연결 역추적 방법.

【청구항 10】

제 9항에 있어서,

상기 (a) 단계는,

(a1) 상기 공격감지신호를 수신하는 단계;

(a2) 상기 IP 주소 및 포트번호를 기초로 상기 공격 패킷 및 상기 제1응답패킷을 파악하는 단계; 및

(a3) 상기 공격패킷 및 상기 제1응답패킷을 차단하는 단계;를 포함하는 것을 특징으로 하는 연결 역추적 방법.

【청구항 11】

제 8항에 있어서,

(e) 외부네트워크로부터 워터마크를 포함하는 패킷을 수신하면 상기 워터마크를 삽입한 외부네터워크의 시스템으로 소정의 탐지패킷을 전송하는 단계를 더 포함하는 것을 특징으로 하는 연결 역추적 방법.

【청구항 12】

제 11항에 있어서,

상기 (e) 단계는,

(e1) 수신한 패킷에 포함된 워터마크를 탐지하는 단계;

(e2) 상기 워터마크를 탐지하면 상기 수신한 패킷의 근원지 및 목적지 IP 주소와 포트 번호를 포함하는 탐지패킷을 생성하는 단계; 및

(e3) 상기 패킷에 상기 워터마크를 최초로 삽입한 외부시스템으로 상기 생성된 탐지패킷을 전송하는 단계;를 포함하는 것을 특징으로 하는 연결 역추적 방법.

【청구항 13】

제 8항에 있어서,

상기 (c) 단계는,

상기 수신한 하나이상의 탐지패킷에 포함된 근원지 및 목적지 IP 주소 및 포트번호를 기초로 공격자시스템의 위치를 역추적하는 단계를 포함하는 것을 특징으로 하는 연결 역추적 방법.

【청구항 14】

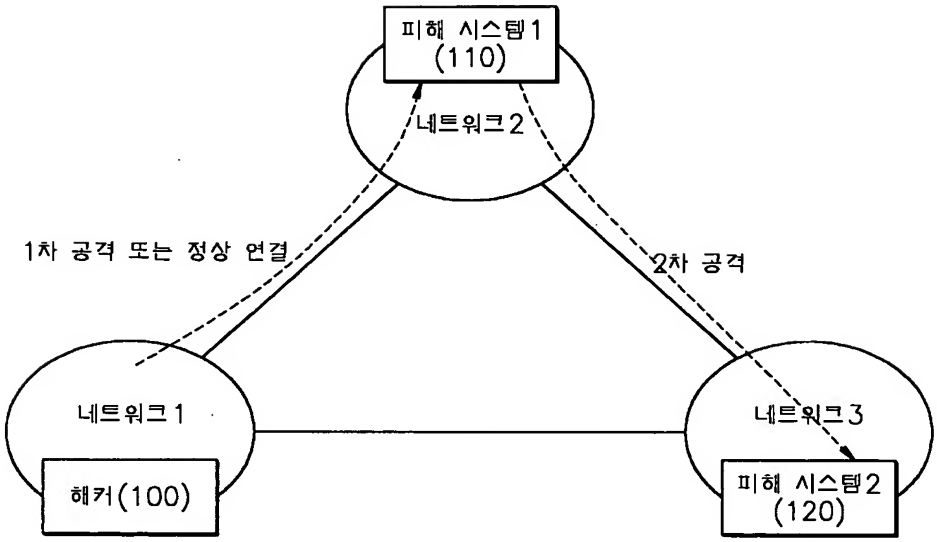
(a) 시스템 침입신호를 수신하면, 상기 시스템으로 전송되는 공격패킷 및 상기 공격패킷에 대한 응신으로 상기 시스템으로부터 출력되는 제1응답패킷을 차단하는 단계;

(b) 상기 공격패킷에 대한 응신으로 워터마크를 삽입한 제2응답패킷을 생성하여 상기 공격패킷의 근원지 주소로 전송하는 단계; 및

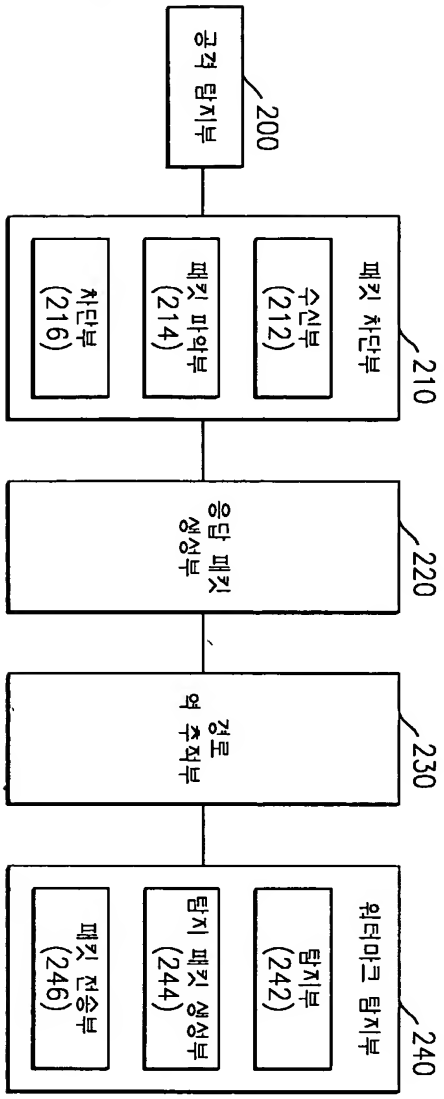
(c) 상기 제2응답패킷이 공격자시스템으로 전송되는 경로상에 존재하는 시스템으로부터 상기 제2응답패킷에 대한 응신으로 하나 이상의 탐지패킷을 수신하고, 상기 탐지패킷을 기초로 상기 제2응답패킷의 전송경로를 역추적하여 상기 공격자시스템의 위치를 파악하는 단계;를 포함하는 것을 특징으로 하는 연결 역추적 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【도면】

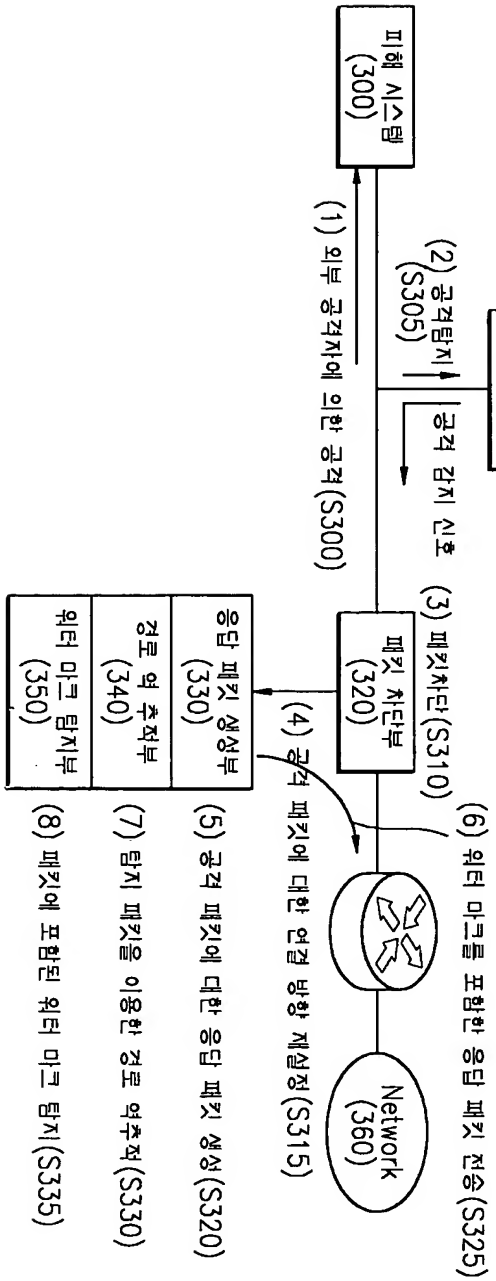
【도 1】


피해 시스템1
(110)
네트워크2
1차 공격 또는 정상 연결
2차 공격
네트워크1
해커(100)
네트워크3
피해 시스템2
(120)

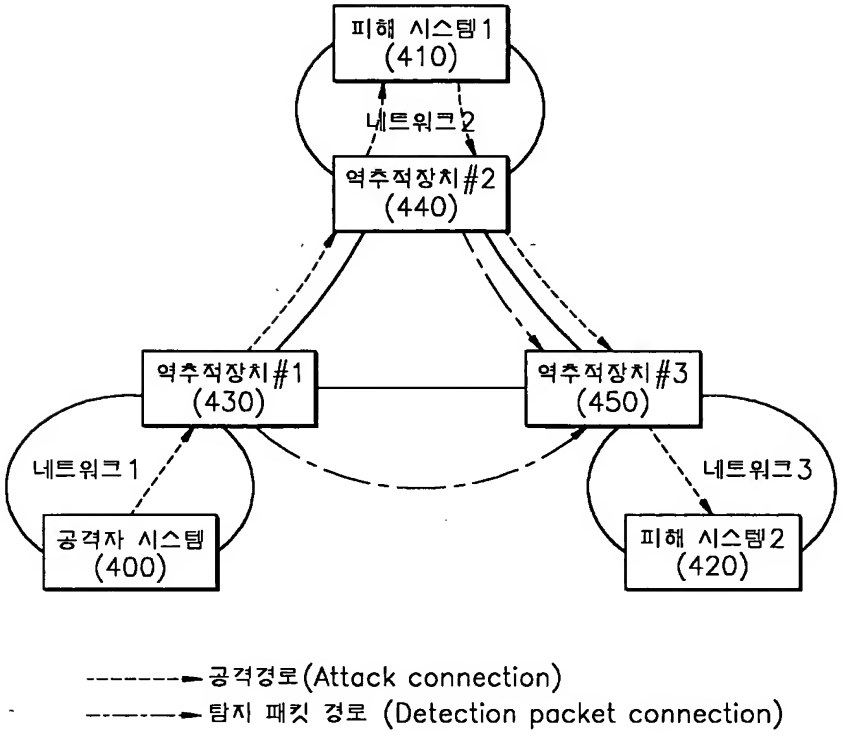
【도 2】


공격 탐지부
200
패킷 차단부
210
수신부 (212)
패킷 파악부 (214)
차단부 (216)
응답 패킷 생성부
220
경로 역 추적부
230
워터마크 탐지부
240
탐지부 (242)
탐지 패킷 생성부 (244)
패킷 전송부 (246)

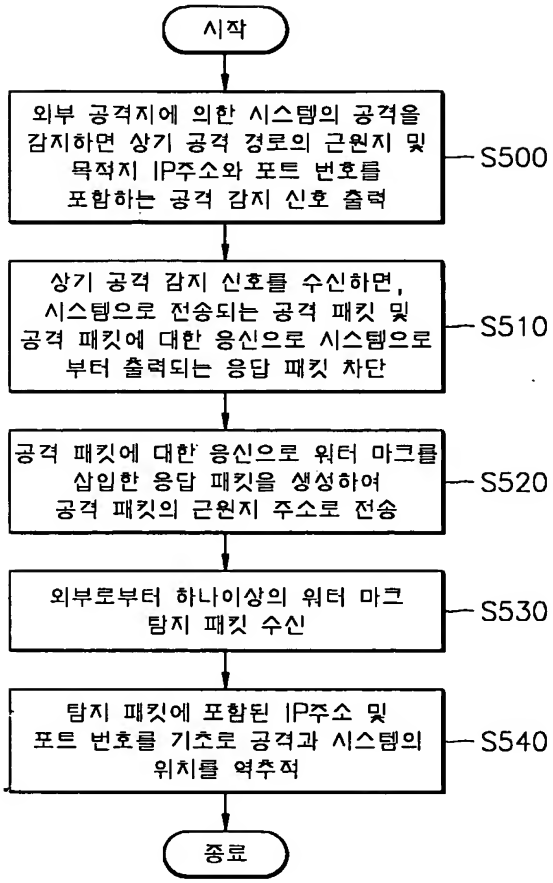
【도 3】


피해 시스템 (300)
(1) 외부 공격자에 의한 공격(S300)
(2) 공격탐지 (S305)
공격 탐지부 (310)
공격 감지 신호
(3) 패킷차단(S310)
패킷 차단부 (320)
(4) 공격 패킷에 대한 연결 방향 재설정(S315)
응답 패킷 생성부 (330)
(5) 공격 패킷에 대한 응답 패킷 생성(S320)
경로 역 추적부 (340)
(7) 탐지 패킷을 이용한 경로 역추적(S330)
워터 마크 탐지부 (350)
(8) 패킷에 포함된 워터 마크 탐지(S335)
(6) 워터 마크를 포함한 응답 패킷 전송(S325)
Network (360)

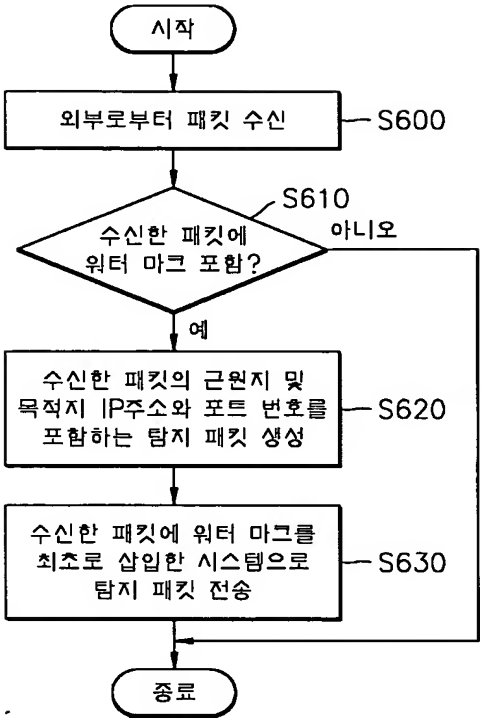
【도 4】


피해 시스템1
(410)
네트워크2
역추적장치#2
(440)
역추적장치#1
(430)
역추적장치#3
(450)
네트워크1
네트워크3
공격자 시스템
(400)
피해 시스템2
(420)
공격경로(Attack connection)
탐지 패킷 경로 (Detection packet connection)

【도 5】


시작
외부 공격지에 의한 시스템의 공격을 감지하면 상기 공격 경로의 근원지 및 목적지 IP주소와 포트 번호를 포함하는 공격 감지 신호 출력
S500
상기 공격 감지 신호를 수신하면, 시스템으로 전송되는 공격 패킷 및 공격 패킷에 대한 응신으로 시스템으로부터 출력되는 응답 패킷 차단
S510
공격 패킷에 대한 응신으로 워터 마크를 삽입한 응답 패킷을 생성하여 공격 패킷의 근원지 주소로 전송
S520
외부로부터 하나이상의 워터 마크 탐지 패킷 수신
S530
탐지 패킷에 포함된 IP주소 및 포트 번호를 기초로 공격과 시스템의 위치를 역추적
S540
종료

【도 6】


시작
외부로부터 패킷 수신
S600
S610
수신한 패킷에 워터 마크 포함?
아니오
예
수신한 패킷의 근원지 및 목적지 IP주소와 포트 번호를 포함하는 탐지 패킷 생성
S620
수신한 패킷에 워터 마크를 최초로 삽입한 시스템으로 탐지 패킷 전송
S630
종료